

Control Plane Snooping implementation report

SAVI-CPS-01

Jun Bi, Jianping Wu, Guang Yao, Fred Baker

IETF75, Stockholm

July 30, 2009

Outline

- Vendor's implementation
- Demonstration
 - Experiments video
 - Onsite demo

Vendors' implementation

- Currently 6 vendors implemented SAVI-CPS in their Ethernet Switches
 - H3C (3Com): S5500EI, S5500SI, S5120EI, E126A, E152, E328, E352
 - ZTE: ZXR10 8900, 5900, 3900A
 - Digital China: DCRS-5950, 3950
 - Ruijie: RG-S8600, S5750, S5760, S2900, S2600
 - Bitway: BitStream 7000, 6000, 3000
 - Centec: E600 and E300
- Cisco, Huawei are also collaborating with CERNET for implementation
- IPv6 Forum IPv6 ready test (BII)

SAVI switch test for 100 campus networks



Current SAVI-CPS Deployment in CERNET2

- SAVI-CPS switches installation
 - H3C (3Com): 10000+ switches in 79 universities
 - Ruijie: 9000+ switches in 91 universities
 - Digital China: 2000+ switches in 26 universities
 - ZTE: 200+ switches in 16 universities
 - Bitway and Centec: in Tsinghua testbed
- To install more in next steps

Demonstration

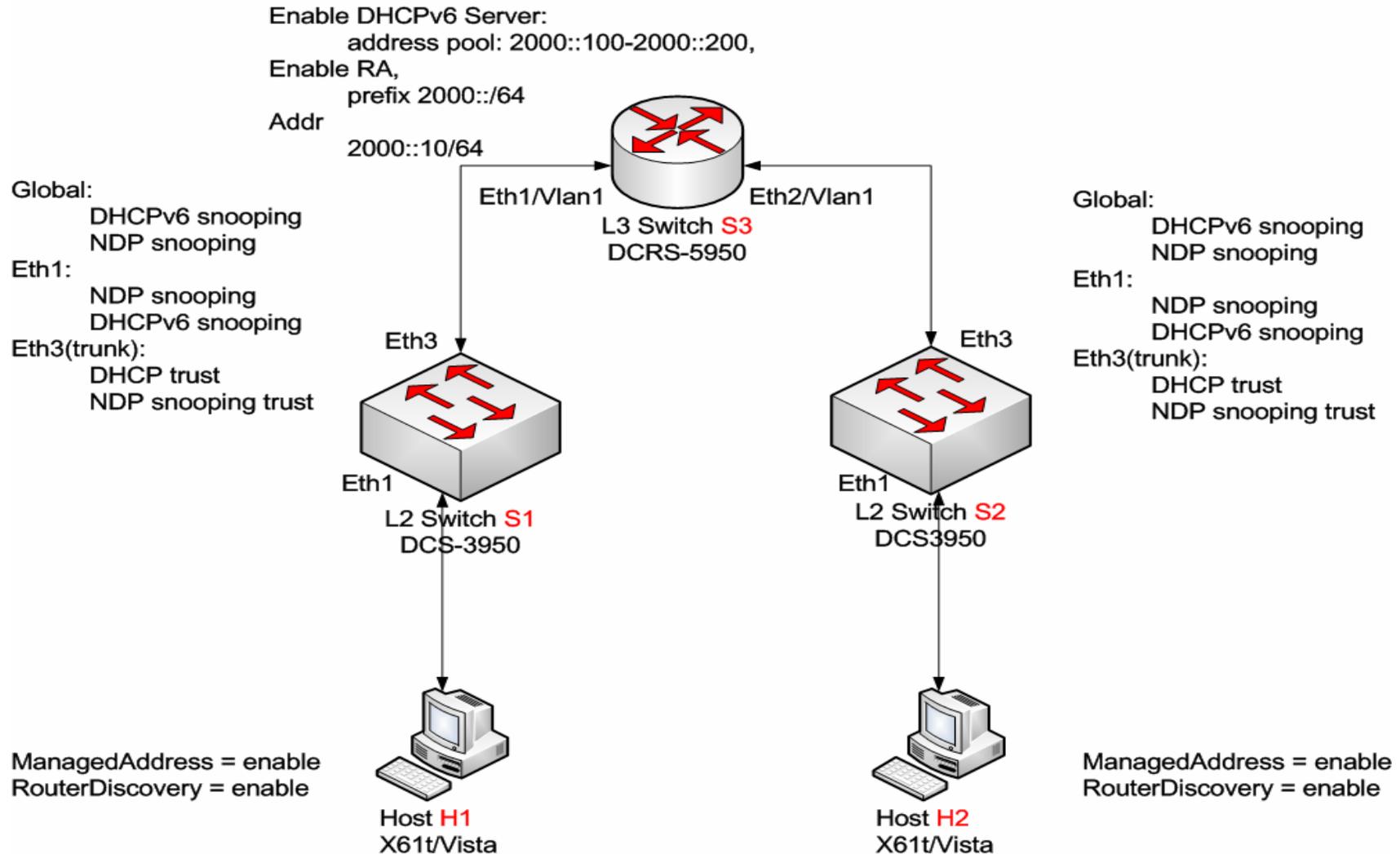
Video on experiments scenarios

- To save the presentation time at SAVI WG meeting, we have recorded video for 13 scenarios
 - Prevent attack against DAD procedure
 - Prevent attack against DAD procedure from undeployed area.
 - Prevent RA spoofing attack
 - Prevent DHCP server spoofing
 - Prevent address exhausting attack
 - Binding in SLAAC and DHCP Co-Existing Environment
 - Host changes port
 - Host changes port across switches
 - Topology Changing (Change port)
 - Topology Changing (Change switch)
 - Switch Reboot
 - DHCPv6 Only Environment
 - Duplicated SLAAC Address
 - To download: <ftp://ietf:ietf@202.112.49.246>

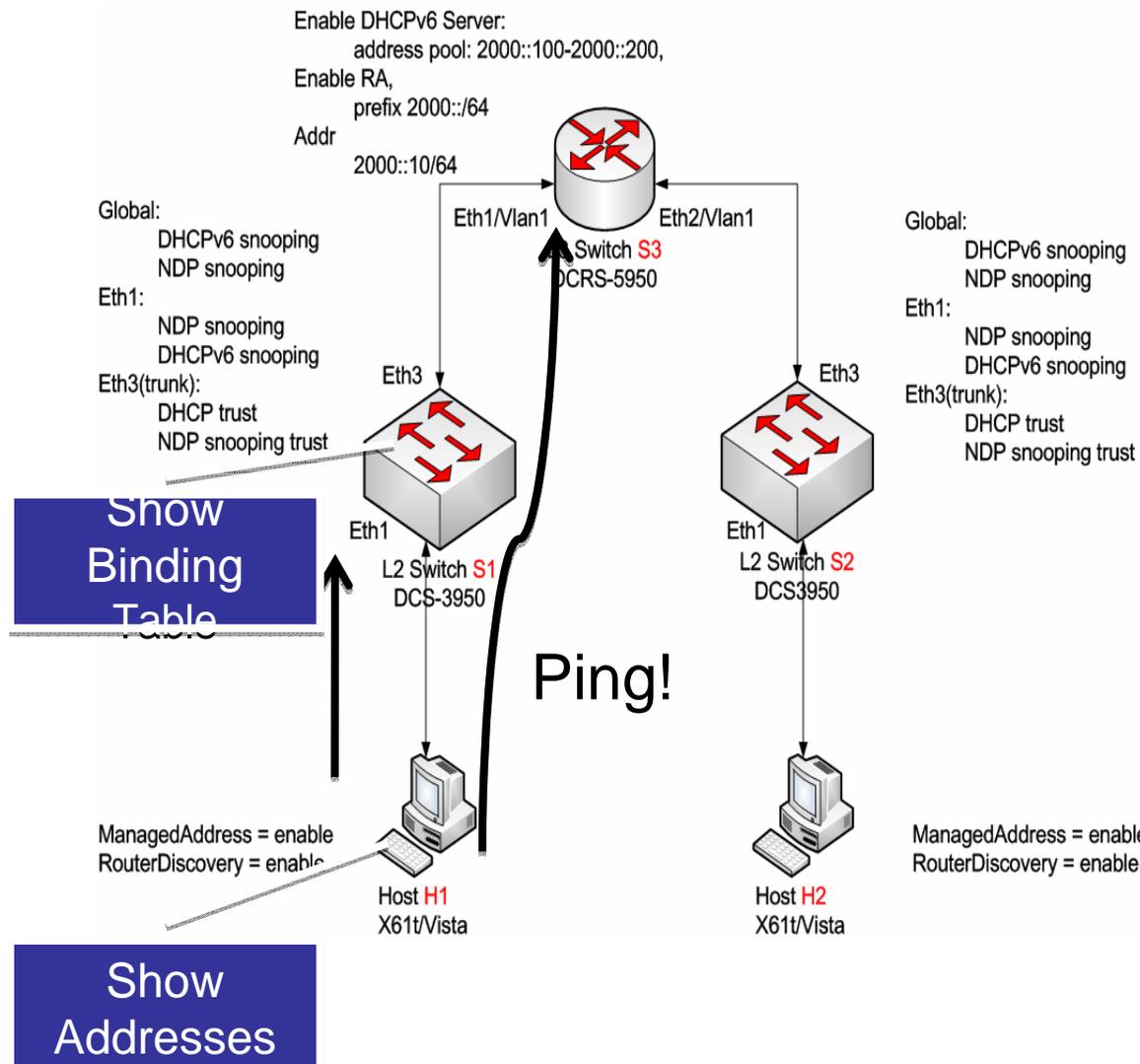
On-Site Demo

- We bring 3 switches at IETF75
 - Set up binding based on Control Packet Snooping in SLAAC and DHCP co-existing environment.
 - Handle SLAAC Address Collision.
 - Handle host change port over switches and DHCP collision.
 - On-site demo is arranged at the end of WG meeting

Topology and Configuration

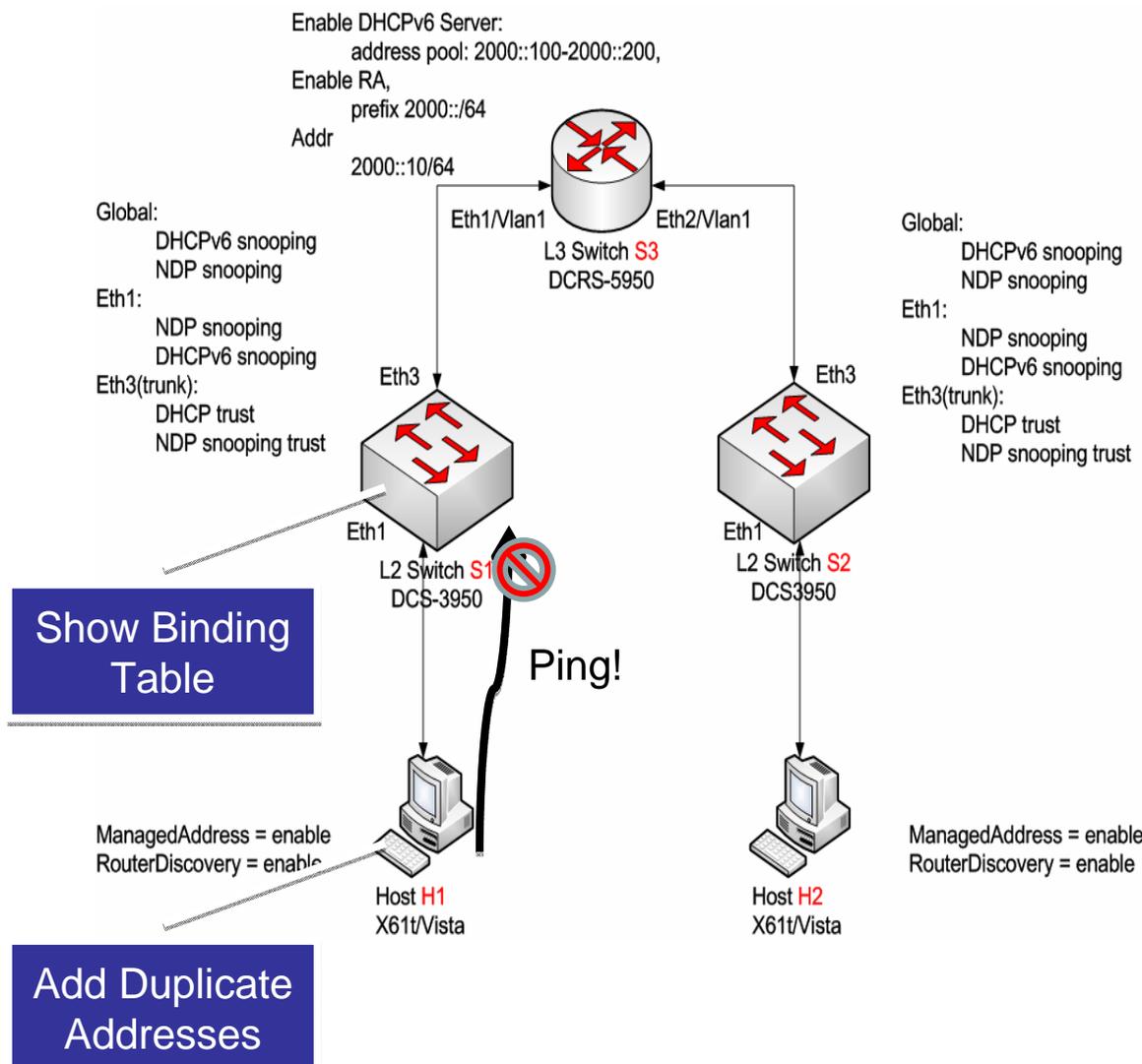


Step 1: Set Up Binding based on Control Packet Snooping



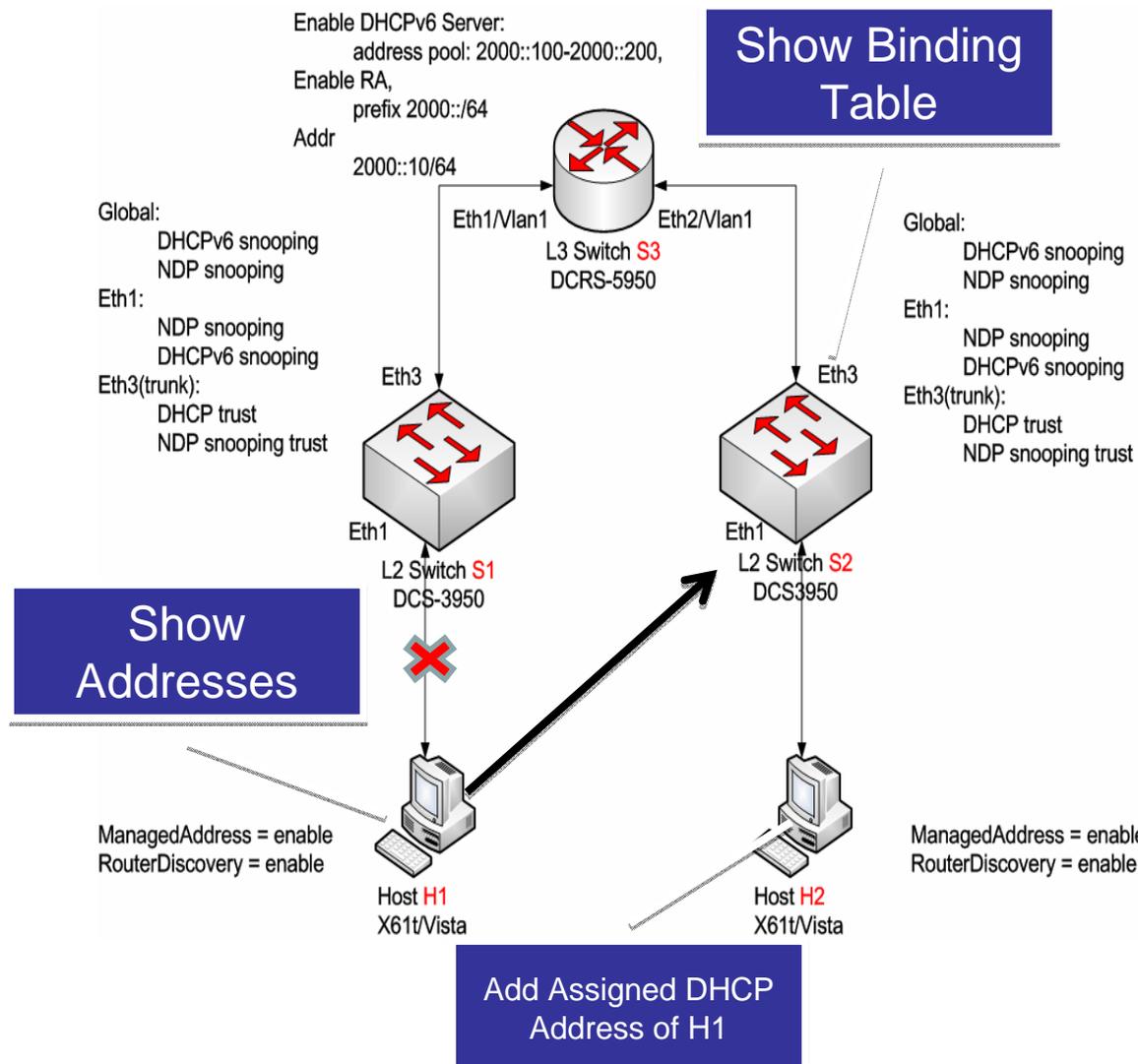
- 1.1 Before H1 connected to S1, show *NDP binding table* and *DHCPv6 binding table* on S1.
- 1.2 Connect H1 to S1.
- 1.3 Show addresses got by H1.
- 1.4 Show *NDP binding table* and *DHCPv6 binding table* on S1.
- 1.5 Ping router address 2000::10 from H1.

Step 2: Not Set Up Binding when SLAAC Addresses Conflict



- 2.1 Manually configure an address **A** of **H2** on **H1**.
- 2.2 Show address state on **H1**.
- 2.3 Show *NDP binding table* on **S1**.
- 2.4 Ping 2000::10 from H1 using address **A**.

Step 3: Change Port accross Switches & DHCP Collision



- 3.1 Disconnect **H1** from **S1**.
- 3.2 Configure the DHCP address got by **H1** on **H2** manually.
- 3.3 Connect **H1** to **Eth2** on **S2**.
- 3.4 Show addresses got by **H1**.
- 3.5 Show *NDP binding table* and *DHCPv6 binding table* on **S2**.

Conclusions

- SAVI-CPS, no known major issues observed
- SAVI-CPS, already implemented by multiple vendors
- SAVI-CPS, based on current test, it's stable
 - Are doing more test in real deployment environment
- SAVI-CPS, is being largely deployed
 - 100 Campus networks, totally 1 Million users
- Propose to adopt SAVI-CPS as SAVI WG Draft (but could be considered in different documents)
- Will do more real work and report in IETF76

Thank You!
Q & A